

Christensen Young & Associates, PLLC
Steven A. Christensen, #5190
Cameron S. Christensen, #16015
9980 South 300 West, Suite 200
Sandy, UT 84070
Phone: 801-676-6447
steven@christensenyounglaw.com
cameron@christensenyounglaw.com
Attorneys for Plaintiff and proposed class

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH**

TAYLOR GIRARD, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

HEALTHEQUITY, INC.,

Defendant.

Case No. 2:24-cv-556

COMPLAINT – CLASS ACTION

JURY TRIAL DEMANDED

Plaintiff Taylor Girard (“Plaintiff”) individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this Class Action Complaint against HealthEquity Inc. (“HealthEquity”). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which is alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted HealthEquity with sensitive personally identifiable information (“PII”)¹ and protected health information (“PHI,” and collectively with PII, “Private

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

Information”), as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), that was subsequently exposed in a data breach, which HealthEquity publicly disclosed on July 26, 2024 (the “Data Breach” or the “Breach”).

2. Plaintiff’s claims arise from Defendant’s failure to properly secure and safeguard Private Information that was entrusted to it as part of Plaintiff’s and Class Members’ receipt of medical services, and its accompanying responsibility to store and transfer that information. More than 4,300,000 consumers were affected by the Data Breach, in which sensitive personal information, including names, dates of birth, addresses, telephone numbers, employee IDs, employers, Social Security Numbers, health card numbers, health plan member numbers, dependent contact information, HealthEquity benefit type, diagnoses, prescription details, HealthEquity account type, and payment card information, were accessed by an unauthorized third party.²

3. HealthEquity is a healthcare business services company incorporated in Delaware and headquartered in Draper, Utah.³ HealthEquity serves as the custodian of Health Savings Accounts (“HSA”) and other similar types of accounts.⁴

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

² *Data Breach Notification: HealthEquity, Inc.*, OFFICE OF THE MAINE ATTORNEY GENERAL (July 26, 2024) <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=773> (last visited August 2, 2024).

³ *Notice of Data Breach*, HEALTHEQUITY, <https://www.healthequity.com/breach> (last visited August 2, 2024).

⁴ *Id.*

5. On or around March 25, 2024, HealthEquity received an alert describing a possible data security incident.⁵ In response, HealthEquity secured its network and then launched an investigation to learn more about the incident and whether any consumer information may have been impacted.⁶

6. On June 10, 2024, HealthEquity completed its investigation, confirming that an unauthorized party had been able to access certain consumer data.⁷

7. On July 26, 2024, HealthEquity filed its first public notice of the Data Breach.⁸

8. Plaintiff's claims arise from Defendant's failure to safeguard Private Information provided by, and belonging to, its customers and failure to provide timely notice of the Data Breach.

9. Defendant failed to take precautions designed to keep its customers' Private Information secure.

10. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information that it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

11. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

12. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have

⁵ *Data Breach Notification: HealthEquity, Inc.*, OFFICE OF THE MAINE ATTORNEY GENERAL (July 26, 2024) <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=773> (last visited August 2, 2024).

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Private Information for Plaintiff and Class Members.

14. As a result of the Defendant's inadequate digital security and notice process, Plaintiff and Class Members' Private Information was exposed to criminals. Plaintiff and the Class have suffered and will continue to suffer injuries including financial losses caused by misuse of Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

15. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach.

16. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence per se; and unjust enrichment.

17. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and

stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

18. Plaintiff Taylor Girard is a resident and citizen of Lafayette, Louisiana. Plaintiff is an employee of Florida Blue and has an HSA through her employer that is administered by HealthEquity. Since March 25, 2024, Plaintiff has received an uptick in spam messages. Moreover, in May 2024, Plaintiff was the victim of a series of fraudulent transactions. Plaintiff had approximately a dozen charges in excess of \$1,000 made from her HSA card that she reported as fraud. Upon review, the charges were deemed fraudulent. As a consequence of the Data Breach, Plaintiff has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of identity fraud. As a result of the Data Breach, Plaintiff is now subject to substantial and imminent risk of future harm. Plaintiff would not have enrolled in a HealthEquity managed HSA had she known that it would expose her sensitive Private Information.

Defendant

19. HealthEquity is a healthcare business services company incorporated in Delaware and headquartered at 15 West Scenic Pointe Dr., Suite 100, Draper, Utah 84020 .⁹ HealthEquity serves as the custodian of Health Savings Accounts and other similar types of accounts.¹⁰ HealthEquity is the parent corporation of WageWorks, Inc. and Further Operations LLC.¹¹

⁹ *Our Company*, HEALTHEQUITY, <https://www.healthequity.com/about> (last visited August 2, 2024)

¹⁰ *Id.*

¹¹ *Data Breach Notification: HealthEquity, Inc.*, OFFICE OF THE MAINE ATTORNEY GENERAL (July 26, 2024) <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=773> (last visited August 2, 2024).

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class Members.

21. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in Draper, Utah.

22. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background on Defendant

23. Defendant is a healthcare business services company that serves as the custodian of HSA's and other similar types of accounts.¹²

24. In the ordinary course of its business practices, Defendant stores, maintains, and uses individuals' Private Information, including Plaintiff's and Class Members', information, *inter alia*: names, dates of birth, addresses, telephone numbers, employee IDs, employers, Social Security Numbers, health card numbers, health plan member numbers, dependent contact information, HealthEquity benefit type, diagnoses, prescription details, HealthEquity account type, and payment card information, were accessed by an unauthorized third party.¹³

25. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the Private Information collected from

¹² *Id.*

¹³ *Notice of Data Breach*, HEALTHEQUITY, <https://www.healthequity.com/breach> (last visited August 2, 2024).

them would be kept safe, confidential, that the privacy of that information would be maintained.

26. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

The Data Breach

28. On or around March 25, 2024, HealthEquity received an alert describing a possible data security incident.¹⁴ In response, HealthEquity secured its network and then launched an investigation to learn more about the incident and whether any consumer information may have been impacted.¹⁵

29. On June 10, 2024, HealthEquity completed its investigation, confirming that an unauthorized party had been able to access certain consumer data.¹⁶

30. HealthEquity's investigation determined that an unauthorized actor may have obtained consumers sensitive Private Information including names, dates of birth, addresses, telephone numbers, employee IDs, employers, Social Security Numbers, health card numbers, health plan member numbers, dependent contact information, HealthEquity benefit type, diagnoses, prescription details, HealthEquity account type, and payment card information, were

¹⁴ Phil Muncaster, *HealthEquity Breach Hits 4.3 Million Customer*, INFOSECURITY MAGAZINE (July 30, 2024) <https://www.infosecurity-magazine.com/news/healthequity-breach-43-million/> (last visited August 2, 2024).

¹⁵ *Id.*

¹⁶ *Id.*

accessed by an unauthorized third party.¹⁷ HealthEquity first publicly disclosed the Data Breach on July 26, 2024.¹⁸

31. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive personal information of Plaintiff and Class Members.

32. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and illegally used in the future.

Defendant's Failure to Prevent, Identify and Timely Report the Data Breach

33. Defendant admits that an unauthorized third party accessed its network systems in order to obtain sensitive information about its current and former customers.

34. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

35. Defendant was not only aware of the importance of protecting the Private Information that it maintains, as alleged, it promoted its capability to do so, as evident from its Privacy Policy.¹⁹

36. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

¹⁷ Notice of Data Breach, HEALTHEQUITY, <https://www.healthequity.com/breach> (last visited August 2, 2024).

¹⁸ Data Breach Notification: HealthEquity, Inc., OFFICE OF THE MAINE ATTORNEY GENERAL (July 26, 2024) <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=773> (last visited August 2, 2024).

¹⁹ HealthEquity, Inc. Privacy Notice, HEALTHEQUITY, https://www.healthequity.com/doclib/general/gen_privacy_notice.pdf (last visited August 2, 2024).

37. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC’s data security principles and practices,²⁰ Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present customers’ sensitive personal information.

38. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.²¹ Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

39. Despite this guidance, Defendant delayed the notification of the Data Breach. Based on HealthEquity’s filing with the Office of the Maine Attorney General, the Data Breach is believed to have occurred on or around March 25, 2024, yet, by its own admission, Defendant did not issue a public notice until July 26, 2024, and has not begun to issue notice letters to impacted consumers.²²

The Harm Caused by the Data Breach Now and Going Forward

40. Victims of data breaches are susceptible to becoming victims of identity theft.

41. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority,” 17 C.F.R. § 248.201(9), and when “identity thieves have your personal information, they can drain your bank account, run up charges

²⁰ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited August 2, 2024).

²¹ *Id.*

²² *Data Breach Notification: HealthEquity, Inc.*, OFFICE OF THE MAINE ATTORNEY GENERAL (July 26, 2024), <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=773> (last visited August 2, 2024).

on your credit cards, open new utility accounts, or get medical treatment on your health insurance.”²³

42. The type of data that was accessed and compromised here – such as full names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

43. Plaintiff and Class members face a substantial risk of identity theft given that their Social Security numbers, addresses, phone numbers, dates of birth, health insurance information and other important Private Information were compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

44. Stolen Private Information is often trafficked on the “dark web,” a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the “dark web” due to this encryption, which allows users and criminals to conceal their identities and online activity.

45. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.²⁴

²³ *Prevention and Preparedness*, NEW YORK STATE POLICE, <https://troopers.ny.gov/prevention-and-preparedness> (last visited August 2, 2024).

²⁴ *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring> (last visited August 2, 2024).

46. For example, in one recent case unsealed by the U.S. Department of Justice, an Illinois man led a group of criminals in marketing almost 50,000 stolen payment cards on dark web marketplaces, generating at least \$1 million in cryptocurrency.²⁵

47. Private Information remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, someone can purchase a full range of documents that will allow identity theft, including \$500 for a high-quality U.S. driver's license, \$25 for a hacked social media account, \$110 for credit card information, and \$150 for banking account information.²⁶

48. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."²⁷

49. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained:

²⁵ *Is Your Information for Sale on the Dark Web?*, NASDAQ VERAFIN (Feb. 26, 2024) <https://verafin.com/2024/02/is-your-information-for-sale-on-the-dark-web/> (last visited August 2, 2024).

²⁶ Ryan Smith, *Revealed – how much is personal information worth on the dark web?* (May 1, 2023) <https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx> (last visited August 2, 2024).

²⁷ *Id.*

“[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market.”²⁸

50. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to individuals and business victims.²⁹

51. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”³⁰ Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

52. As a result of the Data Breach, the Private Information of Plaintiff and Class Members have been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered thereby as a direct result of Defendant’s Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their

²⁸*Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) <https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security> (last visited August 2, 2024).

²⁹ *2019 Internet Crime Report Released*, FBI, <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in.%2Ddelivery%20scams%2C%20and%20e%20xtortion> (last visited August 2, 2024).

³⁰ *Id.*

personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' Private Information.

53. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

54. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

55. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for

which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

56. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in July of 2024 (the “Class”).

57. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge’s immediate family.

58. Plaintiff reserves the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

59. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

60. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiff estimates that the Class is comprised of hundreds of thousands of Class Members. The Class is sufficiently numerous to warrant certification.

61. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because, Plaintiff, like the Class Members, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members that was caused by the same misconduct by Defendant.

62. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

63. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

64. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

- a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- c. Whether Defendant's storage of Plaintiff's and Class Members' Private Information was done in a negligent manner;

- d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;
- e. Whether Defendant's conduct was negligent;
- f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;
- g. Whether Defendant took sufficient steps to secure its customers' Private Information;
- h. Whether Defendant was unjustly enriched;
- i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

65. Information concerning Defendant's policies is available from Defendant's records.

66. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

67. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

68. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

69. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of Plaintiff and All Class Members)

70. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

71. Plaintiff brings this claim individually and on behalf of the Class Members.

72. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

73. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

74. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

75. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its customers' Private Information.

76. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a

position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

77. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

78. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

79. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
and
- c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

80. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

81. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

82. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

83. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry

guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

84. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

85. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

86. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

87. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

88. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

89. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members

have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II

Negligence *Per Se* (On Behalf of Plaintiff and All Class Members)

90. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

91. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff’s and Class Members’ Private Information. Various FTC publications and orders also form the basis of Defendant’s duty.

92. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff’s and Class Members’ Private Information and not complying with industry standards.

93. Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

94. Defendant violation of Section 5 of the FTC Act constitutes negligence per se.

95. Class members are consumers within the class of persons Section 5 of the FTC Act

were intended to protect.

96. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

97. As a result of Defendant's negligence, Plaintiff and the other Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

98. Plaintiff incorporates by reference and re-allege each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

99. Plaintiff and Class Members conferred a benefit upon Defendant by using Defendant's services.

100. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's Private Information, as this was used for Defendant to administer its services to Plaintiff and the Class.

101. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class Members' services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the

proposed Class would not have provided their Private Information to Defendant or utilized their services had they known Defendant would not adequately protect their Private Information.

102. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it because of its misconduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representatives of the Class and his counsel as Class Counsel;
- (b) For an order declaring the Defendant's conduct violates the laws referenced herein;
- (c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (d) For damages in amounts to be determined by the Court and/or jury;
- (e) An award of statutory damages or penalties to the extent available;
- (f) For pre-judgment interest on all amounts awarded;
- (g) For an order of restitution and all other forms of monetary relief; and
- (h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 2, 2024

Respectfully submitted,

By: /s/Steven A. Christensen

Steven Christensen

Cameron Christensen

CHRISTENSEN YOUNG & ASSOCIATES

9980 South 300, West Suite 200

Sandy, Utah 84070

Telephone: (801) 676-6447

Facsimile: (888) 569-2786

Email: steven@christensenyounqlaw.com

cameron@christensenyounqlaw.com

Courtney E. Maccarone

LEVI & KORSINSKY, LLP

33 Whitehall Street, 17th Floor

New York, NY 10004

Telephone: (212) 363-7500

Facsimile: (212) 363-7171

Email: cmaccarone@zlk.com

Proposed Class(es)

**Pro Hac Vice Forthcoming f*